SYNOPSIS

Ph.D in Computer Science

PERFORMANCE EFFICIENT METHODS TO HANDLE ZERO-DAY ATTACKS IN CLOUD ENVIRONMENT

By

SWATHY AKSHAYA

(17PHCSF003)

Supervisor

Dr. G. PADMAVATHI

Department of Computer Science

Submitted to

Avinashilingam Institute for Home Science and Higher Education for Women,
Coimbatore - 641 043

AUGUST 2025

1. Introduction

A zero-day attack is a type of cyber-attack that exploits a previously unknown vulnerability in a software application or a system. These attacks are called "zero-day" because the software developer has zero days to address the vulnerability since it has just been discovered [1]. The term zero-day attack refers to a single or specific instance of an attack exploiting a newly discovered vulnerability, whereas zero-day attacks refers to multiple instances of such attacks or the general concept of attacks exploiting zero-day vulnerabilities stated by Leyla Bilge et al. [1]. To identify a zero-day attack, one would need to find vulnerabilities in software applications or systems before attackers discover them. It can be done through various methods such as code analysis, vulnerability scanning, penetration testing, and threat intelligence [2]. Out of these methods, threat intelligence is gaining improved performance due to the AI (Artificial Intelligence) driven security solutions. The threat of zero-day attacks has become increasingly significant in recent years, as cybercriminals are continually searching for vulnerabilities to exploit. These attacks can cause severe damage to organizations, including data theft, financial loss, and reputational damage. To combat these threats, researchers and practitioners have been exploring various methods for predicting and preventing zero-day attacks [3].

The research proposal outlines a four-phase methodology for predicting zero-day attacks by combining machine learning and deep learning techniques. The first phase employs an Enhanced BPNN with CloudSim simulator to map the attack paths. In subsequent phases, data is systematically preprocessed**,** feature selection is performed, and multiple ML (Machine Learning) / DL (Deep Learning) models are trained and evaluated**,** followed by a comparative analysis of results across approaches. The objective is to proactively suggest performance efficient methods to identify and predict previously unseen (zero-day) threats, enabling organizations to detect attacks before they manifest. This approach proves to enhance the accuracy and reliability of intrusion detection systems by leveraging both traditional machine learning and advanced deep neural network methods, ultimately improving protection of digital assets through early, learned prediction of emerging threats. The research is conducted using a combination of simulation and real-world data to evaluate the proposed models performance. The simulation is performed using CloudSim, synthetic datasets Dataset 1 (Path Dataset) and Dataset 2 (Attack Dataset) is obtained from actual zero-day attack. The results of the comparative analysis will provide insights into the effectiveness of the proposed methodology and its potential for practical applications in cyber security.

Phase 1 is dedicated to identify the potential paths through which a zero-day attack can infiltrate the system. This phase traces the attack path in the cloud environment using a Probabilistic Graph Approach combined with an Enhanced Back Propagation Neural Network (BPNN), supported by Improved Decision Trees (DT) and Weighted K-Means clustering. Outcomes include improved accuracy by 3.01%, precision by 2.63%, recall by 2.27%, and F1-

score by 2.34% compared to Bayesian, Scalable Bayesian, and Probabilistic Bayesian models. Phase 2 employs a hybrid method of Game Theory based on the Nash Equilibrium and an Adaptive Gaming Model based on a Modified Bi-Directional Long Short-Term Memory (LSTM) network to predict zero-day attacks. It enhances the ability to predict the potential zero-day threats within the system through enhanced accuracy prediction, system performance and improved communication between security components achieving up to 11.4% higher accuracy, 11.3% higher precision, 5.5% higher recall, and 5.4% higher F1-score compared to DT, SVM, GNB, and Logistic Regression. Phase 3 propose a Residual Network integrated Deep-Convolutional Zero-Day Adversarial Safety Network, designed for live zero-day attacks. It uses deep learning over the cloud communication network traffic analyzing and detecting events given in Dataset 1 (Path Dataset) and Dataset 2 (Attack Dataset) for real-time anomalies. Advanced convolutional layers and residual connections enhance generalization and classification up to 12.4% higher accuracy, 10.2% higher precision, 9.1% higher recall, and 9.2% higher F1-score over HMM, and up to 9.7% higher accuracy and 10.8% higher recall and ensure faster learning to identify zero-day attacks effectively compared to Bayesian GNN, BERT, TransVAE, and HADE-SVM models. Phase 4 presents an OLFFOA-optimized hybrid deep learning model. This comparative analysis allows for evaluating different models to determine the most efficient and accurate approach for zero-day attack prediction. The model achieves up to 98.1% accuracy, 95.2% precision, 94.4% recall, and 94.8% F1-score on Dataset 2, outperforming ResNet50, CNN-LSTM, and Bi-LSTM individually by 1.9% – 3.1%. The results show improved recognition rates, fewer false positives, and minimized time complexity, thus making the prediction models credible and scalable. Overall, this research work recommends performance efficient methods to handle zero-day attacks in cloud environment. The results are evident when tested with simulated dataset and benchmark dataset in zero-day attack.

2. Recent Statistics of Zero-Day Attack

The following paragraph presents the recent statistics of zero-day attack justifying the need for recommendation of performance efficient methods to handle zero-day attack in cloud.

i. Growing Zero Day Exploits: The zero-day vulnerabilities exploited in the wild have dramatically increased per Mandiant report in 2023, where 55 zero-day vulnerabilities were exploited in 2022 and only 30 in 2021. This is part of a broader trend, showing zero-day vulnerabilities have doubled over the past five years.
ii. Economic Impact: The Ponemon Institute indicates that in 2023, a data breach's average cost is $4.45 million. Zero-day attacks are part and parcel of that. Much of that expense, for detection and response happened - organizations inform that they took weeks, sometimes months, to identify and contain such an attack.
iii. Cloud Security Risks: According to a 2023 survey of Orca Security, 78 percent of the cloud infrastructure security incidents were related to software vulnerabilities that had not been patched, and many of them were exploited by zero-day attacks. Zero-day attacks

within such environments are witnessing exponential growth with large-scale cloud adoption.

iv. Recent Patch Timelines: A 2023 Verizon Data Breach Investigations Report indicates that 49% of the exploited vulnerabilities are still unpatched 30 days following discovery. For zero days, the patch timeline is longer because, at that time, the flaw has not been discovered and, thus, will only be known after the attack occurs. In this case, the systems are left open to those who exploit such a flaw.

v. Limitation of Machine Learning: Although a couple of machine learning models have been deployed to detect cyber threats, Gartner believed that 60% of security professionals claimed that they cannot address complex and changing threats, which are zero-day attacks. The existing ML models are primarily inaccurate, increase false positives, and lack adaptability in the presence of new attacks.

Need for a New Approach

Against this frightening backdrop, it is evident that the more traditional responses in cybersecurity will not help to contain the current onslaught of zero-day attacks, the better part of which utilize sophisticated methods that zero in on their targets. In that case, the world needs the most to prevent these attacks. It is a predictive model that can exploit ML and DL techniques for forecasting, identifying, and eventually alleviating a zero-day attack before its far-reaching consequences are unleashed.

The proposed four-phase methodology addresses the above limitations through its multifaceted, predictive approach that recommends the desirable models to improve the accuracy of detection, prediction, and prevention of zero-day attacks in cloud environments. Advanced techniques, which include those applied in the Probabilistic Graph Approach, Game Theory, and Deep-Convolutional Networks are adopted to provide organizations with robust tools against emerging cyber threats. This would reduce the overall impact of zero-day vulnerabilities on global cybersecurity.

3. Literature Review

This section discusses the significant literatures studied in connection with zero-day attack handling methods. However, it is observed that the significant references for zero-day attack are less, as it is an emerging cyber threat.

Ahmed et al. (2022) employed deep learning techniques that enhanced the accuracy levels of neural networks while detecting botnet attacks. The model was seen to drastically increase the accuracy level with adjustments in the hidden layers of an artificial neural network-based approach. The model clearly showed better performance compared with traditional methods like SVM (Support Vector Machines), NB (Naïve Bayes), and backpropagation

algorithms; it could reach a very high accuracy level of 99.6% for botnet detection. Given that the reliability of the model itself was highly dependent on the availability of a trustworthy dataset, it is not less essential to have deep learning-based applications for cybersecurity than data quality.

The methods described by Sun et al. (2016) are capable of modeling likelihoods of attacks paths in a zero-day attack situation applied in the context of the threat research of networked systems in a probabilistic context, or Bayesian Network. These were intended to reveal object dependencies of the system and any behind the scenes object (links) that was used by an attacker and then provide framework or model the zero-day vulnerabilities. The outputs of their findings showed that uncertainty was easily captured in probabilistic models than deterministic shovel about rule-based models. But they were limited in modeling only stable cloud configurations and they were more likely to send false positive messages - a reason why enhanced methods based on machine learning were necessary.

Scholten (2021) proposed a reliable method that would be applied to predict if an input had the potential to trigger a vulnerability. The study also indicated that vulnerability detection may be made easier based on the historical data that have not been drawn from the user, as it may facilitate smoother identification. A significant drawback identified in this context of approach was that the false positive rate was higher, meaning there had been a compromise concerning efficiency and detection accuracy.

Sun et al. (2018) have come up with the probable methodology through Bayesian Networks of identification of zero-day path in a larger complex system. Modeling of dependency between objects system objects was the focus so as to offer a way to reach concealed paths of attack that can be utilized by unidentified vulnerabilities. The proposed approach allows more accurate formulation of potential zero-day attack paths than deterministic approaches because it allows providing a probabilistic inference process. Nevertheless, scalability was challenged in the paper and so were the misclassification rates in harsh cloud settings; therefore, serving as a source of motivation to conduct more searching high learning initiatives.

Shin et al. (2019) further split the increasing sophistication of network attacks into single-stage and multi-stage attacks. The research outcome indicated that most network attacks are multi-stage designs executed over long periods, making them harder to discover with older security systems. The long-drawn attack patterns of high sophistication require more sophisticated detection systems capable of adapting to increasingly emerging sophisticated attacks in real-time.

Wang et al. (2020) focused on micro-architectural side-channel vulnerabilities (SCAs), allowing attackers to perform sensitive information extraction based on flaws in core performance-enhancing components of systems. In this regard, the authors pointed out how

machine learning algorithms might help to detect such attacks, exploring micro-architectural data to report these attacks. In this regard, the work resulted in a better understanding of the usage of ML for monitoring and detecting hardware-level vulnerabilities, once again emphasizing how detection approaches need to be apt.

Recently, Mishra et al. (2018) published a paper elaborating on the dynamic nature of Intrusion Detection (ID) systems over high-performance computing platforms. Their work pointed to the continuously evolving nature of ID systems as they continually adapt to new functionalities and models to pursue cybersecurity needs. The study aimed to look into how flexible and scalable observation infrastructures could be applied to accommodate dynamic security needs, especially in a setup that deals with large computational workloads.

Emmah et al. (2021) scrutinized the challenges associated with zero-day vulnerabilities, which are security flaws unknown to the software vendor or user. Malware usually exploits these vulnerabilities to stage zero-day attacks. The study and results showed that these vulnerabilities cannot be taken lightly because their existence is unknown, making it an uphill task to mitigate them; traditional methods have no effect on reducing the malware exploitation of these flaws since their entry into the system does not make it obvious. More proactive defense mechanisms are, therefore, necessary.

A new approach to intrusion detection systems using deep learning is proposed by Soltani et al. (2023), which can be adaptive against zero-day attacks. Deep novelty-based classifiers in the domain of network security were developed here. This was novel because it supported deep clustering models with sample generation to improve the framework's ability to detect previously unknown threats. It was one of the first studies applying deep learning to zero-day attack detection, thus opening up further research into AI-driven security solutions. Table 1 represents a small evaluation of the significant literature of zero-day attacks, with their advantages and limitations.

Table 1. Significant Literature of Zero-Day Attacks

Author(s)	Year	Techniques Used	Advantages	Limitations
Yuan Ning, Yufeng Liu, Qiang Ji	2010	Bayesian–BP Neural Network for short-term load forecasting in power systems	Demonstrated hybrid Bayesian + BPNN can enhance prediction accuracy over traditional methods	Domain-specific (power systems); not directly applicable to cybersecurity
Jun Dai, Xiaoyan Sun, Peng Liu	2013	PATROL framework for revealing zero-day attack paths using network-wide system object dependencies	First attempt to trace hidden zero-day paths via dependency graphs; provided practical attack path modeling	High complexity; scalability issues in large dynamic networks
Mikhail Zolotukhin,	2014	Opcode sequence analysis for zero-day	Detected zero-day malware at binary/code level;	Limited to Opcode-based features; may

Timo Hamalainen		malware detection	effective against unknown malware families	fail against obfuscation or polymorphic attacks
Shin et al.	2019	Analysis of multi-stage and single-stage network attacks	Highlights the complexity of modern network attacks	Multi-stage attacks are challenging to detect with traditional security systems
Ahmed et al.	2022	Deep learning with ANN and hidden layer adjustments for botnet detection	Achieved 99.6% accuracy in botnet detection; outperformed SVM, NB, and backpropagation	Model performance is highly dependent on dataset quality
FireEye Mandiant	2023	M-Trends Report on advanced cyber threats (industry insights)	Provided up-to-date global threat intelligence; highlighted surge in zero-day exploits (55 in 2022 vs 30 in 2021)	Industry report; lacks methodological or technical solution details
Ponemon Institute	2023	Global cost analysis of data breaches (IBM Security report)	Highlighted financial/economic impact of zero-day and data breaches ($4.45M avg. cost in 2023)	Focused on cost statistics; does not propose technical mitigation strategies

Research Gaps Identified

Key challenges in zero-day attack includes the following research gaps. Addressing these gaps is essential for a robust zero-day attack detection methodologies and enhancing cybersecurity resilience. Existing methods for zero-day attack detection have an inherent or explicit low accuracy, high false positive classification, and weak prediction, and possible future detection that are unusable for pro-active defense. Additionally, traditional detection models do not ensure detection in real-time nor have the ability to generalize across diverse environments. In addition, to these direct limitations to current detection models, it is common that approaches were poorly optimized or scalable and led to unexpected high false positives and time complexity. Subsequently, this work has contributed to the low accuracy gap using the Enhanced BPNN, by providing an improved prediction via Game Theory - BiLSTM, provided a method to achieve detection in real-time using DC-nZDASN, and made it scalable through the OLFFA-based ensemble model.

a. Limited Availability of Real-World Zero-Day Datasets
b. High False Positive and Negative Rates
c. Inadequate Benchmarking and Standardization
d. Adversarial Vulnerabilities in Prediction Models
e. Poor Domain Generalization and Time Complexity
f. Scalability and Computational Efficiency Concerns
g. Interpretability and Explainability of Detection Models

4. Problem Definition

Based on the above discussions the problem statement is presented as “To devise performance efficient methods to handle zero-day attacks”.

5. Research Objectives

The objectives aim to address critical challenges associated with zero-day attacks in cloud infrastructures. Each phase of the research work is meticulously designed to improve the processes of identification, prediction, detection, and comparative analysis of these advanced threats. By integrating cutting-edge techniques in cyber defense mechanisms the proposed objectives structured according to the research methodology, are as follows.

(i) Enhanced Accuracy, Reduced Misclassification Rates, and Improved Data Security.
(ii) Enhanced Predictability of Zero-Day Attacks, Robust and Accurate, Reliable System Communication.
(iii) Improved Detection of Zero-Day Attacks, Improved Generalization Capacity, Classification Accuracy, and High Detection Efficiency.
(iv) Improved Recognition Rates, Reduced False Positives and Detection Time Complexities.
(v) Mitigation of Zero-Day Attacks in Dynamic Cloud Environment.

6. Research Methodology

The research objectives aim to contribute to the development of more effective and efficient methods for identifying, predicting and detecting zero-day attacks, thereby improving the security of cloud networks and organizations' assets and information. This ultimately suggests the performance efficient methods to handle zero-day attacks in cloud environment. To achieve the given objectives, a four-step methodology is followed. Figure 1 shows the research methodology followed in this thesis.

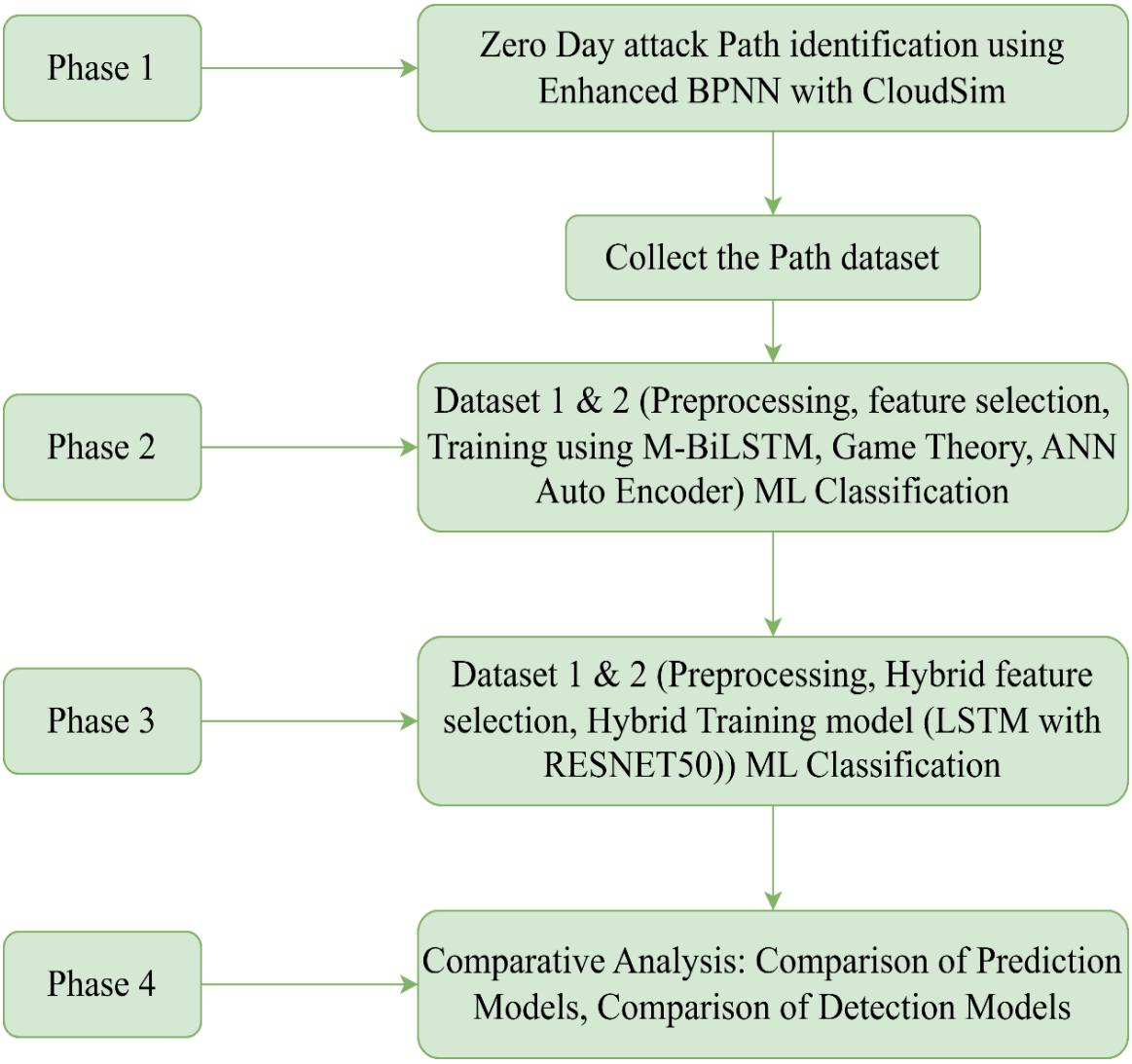
Phase 1
Zero Day attack Path identification using Enhanced BPNN with CloudSim
Collect the Path dataset
Phase 2
Dataset 1 & 2 (Preprocessing, feature selection, Training using M-BiLSTM, Game Theory, ANN Auto Encoder) ML Classification
Phase 3
Dataset 1 & 2 (Preprocessing, Hybrid feature selection, Hybrid Training model (LSTM with RESNET50)) ML Classification
Phase 4
Comparative Analysis: Comparison of Prediction Models, Comparison of Detection Models

Figure 1. Research Methodology of Zero-Day Attack

The proposed methodology is organized into four phases. Phase 1, employing the enhanced BPNN for path identification, followed by Phase 2 focusing on data preprocessing and feature selection techniques. Phase 3 covers model training and testing methods for zero-day attack prediction, while Phase 4 involves optimization techniques to enhance the performance of the models. The framework specifically deals with multiple or several traces of zero-day attacks that are collectively framed in Dataset 1 (Path Dataset) and Dataset 2 (Attack Dataset).

7. Research Contributions

The overall research design and contributions of the thesis is represented in Figure 2.

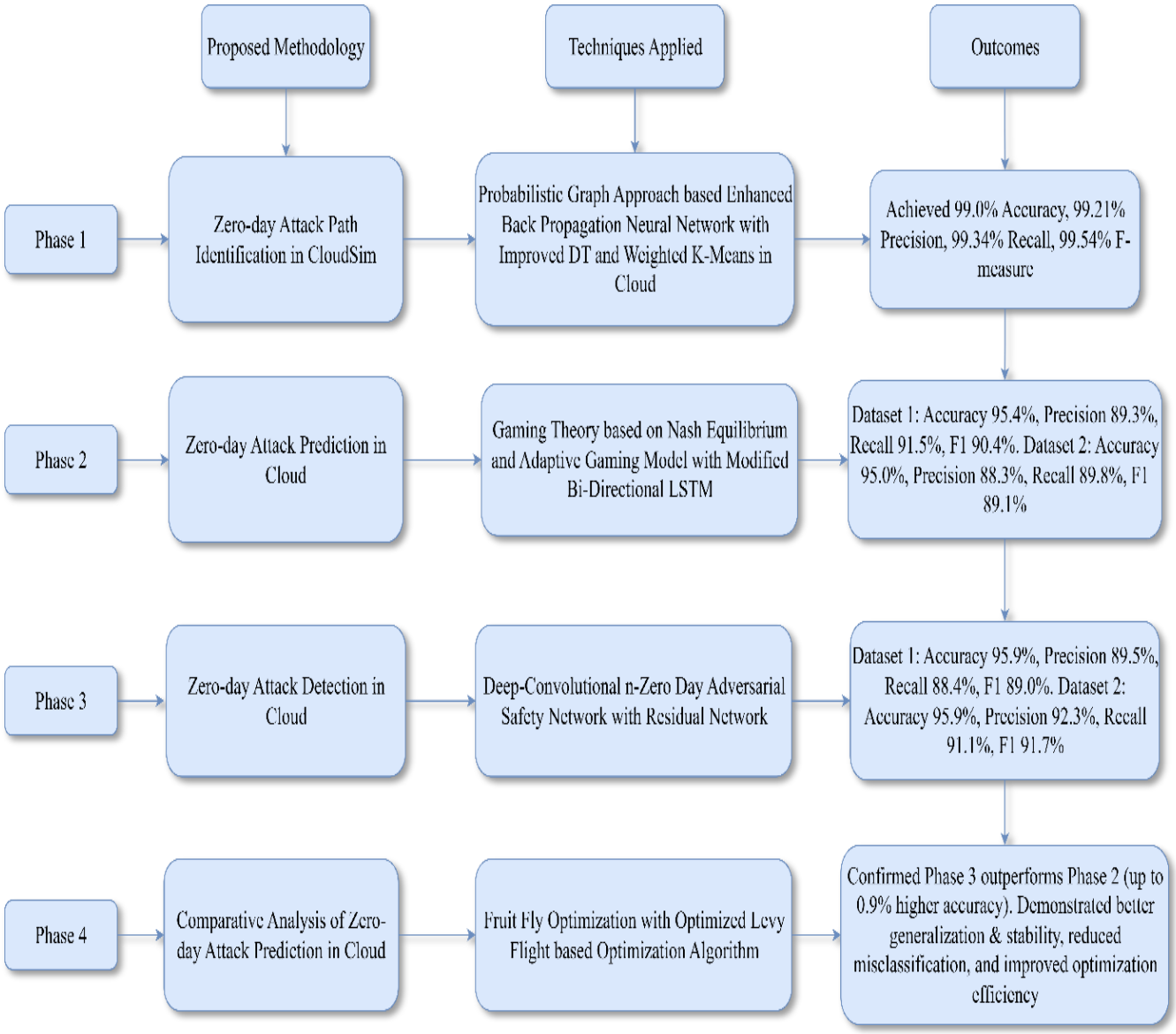
Proposed Methodology
Techniques Applied
Outcomes
Phase 1
Zero-day Attack Path Identification in CloudSim
Probabilistic Graph Approach based Enhanced Back Propagation Neural Network with Improved DT and Weighted K-Means in Cloud
Achieved 99.0% Accuracy, 99.21% Precision, 99.34% Recall, 99.54% F-measure
Phase 2
Zero-day Attack Prediction in Cloud
Gaming Theory based on Nash Equilibrium and Adaptive Gaming Model with Modified Bi-Directional LSTM
Dataset 1: Accuracy 95.4%, Precision 89.3%, Recall 91.5%, F1 90.4%. Dataset 2: Accuracy 95.0%, Precision 88.3%, Recall 89.8%, F1 89.1%
Phase 3
Zero-day Attack Detection in Cloud
Deep-Convolutional n-Zero Day Adversarial Safety Network with Residual Network
Dataset 1: Accuracy 95.9%, Precision 89.5%, Recall 88.4%, F1 89.0%. Dataset 2: Accuracy 95.9%, Precision 92.3%, Recall 91.1%, F1 91.7%
Phase 4
Comparative Analysis of Zero-day Attack Prediction in Cloud
Fruit Fly Optimization with Optimized Levy Flight based Optimization Algorithm
Confirmed Phase 3 outperforms Phase 2 (up to 0.9% higher accuracy). Demonstrated better generalization & stability, reduced misclassification, and improved optimization efficiency

Figure 2. Research Contributions

This research systematically bridges these gaps through a four-phase methodology:

i. Phase 1 improves low accuracy and high false positive issues by using a Probabilistic Graph-based Enhanced BPNN for path identification.
ii. Phase 2 tackles weak predictive capability by integrating Game Theory with a Modified Bi-LSTM and ANN Autoencoder, thereby improving early prediction accuracy and communication between system components.

iii. Phase 3 addresses the lack of real-time detection and adversarial vulnerabilities using a Residual Network–based DC-nZDASN, capable of live traffic anomaly detection with higher resilience.
iv. Phase 4 resolves scalability, optimization, and time-complexity concerns through OLFFOA-driven hyperparameter tuning and Stacking Ensemble learning, while also reducing false positives and improving domain generalization.

a. Limited Availability of Real-World Zero-Day Datasets → Addressed across all phases by combining CloudSim simulated dataset (D1) with Celosia benchmark attack dataset (D2) to balance path-based vulnerabilities and real-world adversarial traces.

b. High False Positive and Negative Rates → Primarily mitigated in Phase 1 (EBPNN) and further reduced in Phase 4 (OLFFOA-Ensemble) through adaptive learning and ensemble decision-making.

c. Inadequate Benchmarking and Standardization → Tackled in Phase 4, where comparative evaluation against multiple baselines (ResNet50, CNN-LSTM, Bi-LSTM, Bayesian, BERT, etc.) ensures standardized benchmarking across datasets and models.

d. Adversarial Vulnerabilities in Prediction Models → Addressed in Phase 3 (DC-nZDASN) through adversarial learning and robust convolutional residual layers that improve resilience against manipulated attack data.

e. Poor Domain Generalization and Time Complexity → Improved in Phase 3 with ResNet50-based feature generalization and further optimized in Phase 4 with OLFFOA to reduce training complexity and ensure domain adaptability.

f. Scalability and Computational Efficiency Concerns → Resolved in Phase 4 by using optimization-driven ensemble learning, ensuring the framework remains scalable to large-scale cloud deployments.

g. Interpretability and Explainability of Detection Models → Partially addressed across Phases 1–4 through model comparison and performance evaluation; however, this remains a future scope where explainable AI (XAI) methods can provide deeper interpretability.

8. Experimental Results and Analysis

This section presents the experimental results obtained from the proposed methodology across the four phases. Each phase's performance metrics are summarized in tables and discussed in detail to highlight the techniques' effectiveness.

Phase 1: Zero-Day Attack Path Identification Using Probabilistic and Graph Approach-Based Back Propagation Neural Network in Cloud

In this phase, the proposed probabilistic graph-based Enhanced Back Propagation Neural Network (EBPNN) introduces a novel approach for identifying, zero-day attack paths in cloud environment. It is necessary to understand how potential attacks might navigate the complex infrastructures of the cloud. The Enhanced BPNN is mainly compared to Bayesian based models because Bayesian Networks represent the established baseline for zero-day attack path findings from the prior works in this area. Bayesian and Probabilistic Bayesian methods are heavily used to track potential zero-day paths so this approach is considered to be the absolute leading methods in the field. The weaknesses of these models included static misclassifications, reduced scalability, or limited to more static and less dynamic cloud infrastructures. By representing attack chains as instance graphs and integrating the adaptive learning capabilities of EBPNN, the model enables systematic visualization of multi-stage attacks and real-time inference without relying on prior attack signatures. Experimental validation demonstrates the proposed method significantly improves the efficiency, accuracy, correctness of identifying potential attack paths with lower rates of misclassification using improved decision trees and weighted K-Means and predictive capability compared to baseline intrusion detection systems, particularly in cloud environment where attack surfaces are highly dynamic. The combination of graph-amplified learning with neural inference enhances both adaptability and proactive defense, establishing the proposed methodology as an intelligent and scalable solution for forecasting and mitigating the evolving zero-day threats.

The insights identified lay the foundations for developing prediction and detection models effectively and ensure that the security model proposed is proactively robust against cyber threats.

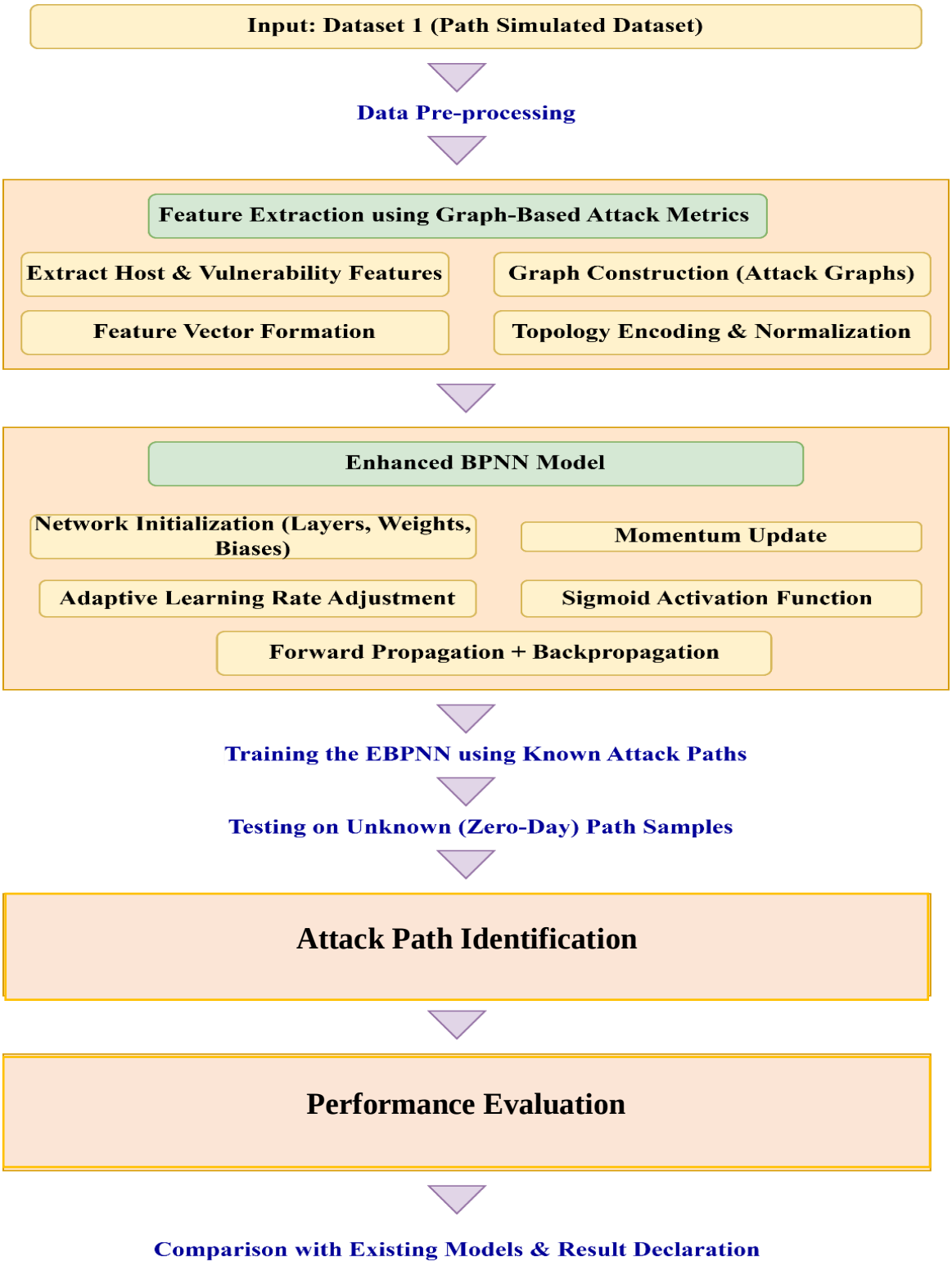
Input: Dataset 1 (Path Simulated Dataset)
Data Pre-processing
Feature Extraction using Graph-Based Attack Metrics
Extract Host & Vulnerability Features
Graph Construction (Attack Graphs)
Feature Vector Formation
Topology Encoding & Normalization
Enhanced BPNN Model
Network Initialization (Layers, Weights, Biases)
Momentum Update
Adaptive Learning Rate Adjustment
Sigmoid Activation Function
Forward Propagation + Backpropagation
Training the EBPNN using Known Attack Paths
Testing on Unknown (Zero-Day) Path Samples
Attack Path Identification
Performance Evaluation
Comparison with Existing Models & Result Declaration

Figure 3. Proposed Framework of Zero Day Attack Path Identification in Phase 1

Figure 3. illustrates a cyberattack detection process using an Enhanced Backpropagation Neural Network (EBPNN), where graph-based features like topology and vulnerabilities are extracted from network traffic logs. These features are input into the EBPNN, which is trained on known attack routes and tested on zero-day samples, producing confidence scores and path probabilities. The model's performance is evaluated using metrics such as accuracy, precision, recall, and false alarm rate, and compared with existing methods for effectiveness.

Table 2. Comparison of BPNN Performance Improvements

Methods	Algorithm	Accuracy	Precision	Recall	F-measure
Existing	Bayesian	96.11	96.67	97.14	97.27
	Scalable Bayesian	97.12	97.27	97.47	98.38
	Probabilistic Bayesian-Network	98.20	98.22	98.21	98.95
Proposed	**EBPNN**	**99.00**	**99.21**	**99.34**	**99.54**

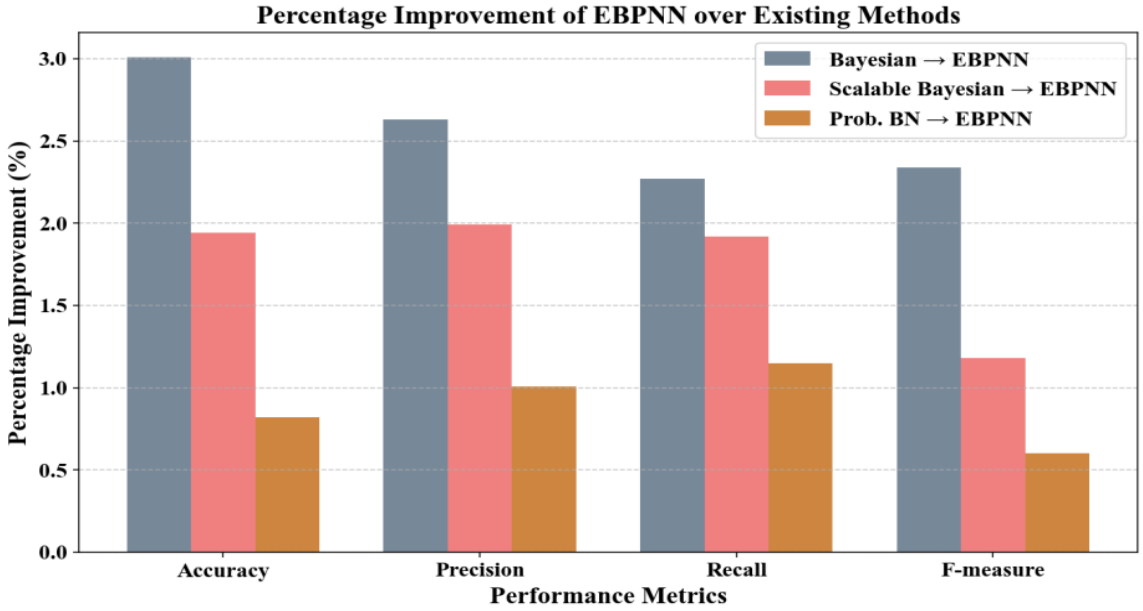

Figure 4. Performance Improvement Comparison Chart

Table 2 and Figure 4. Illustrate the relative improvement of EBPNN compared to the existing methods. The Enhanced Back Propagation Neural Network (EBPNN) demonstrates superior performance over current Bayesian models, achieving up to 3.01% improvement in accuracy and 2.63% in precision. It consistently outperforms advanced models such as Probabilistic Bayesian Networks across all evaluation metrics, highlighting its strength and efficiency in identifying zero-day attack paths. However the identified attack path contains both zero day and non-zero day exploits. Therefore, it is essential to predict only zero day attacks in the path identified.

Dataset Description

In this research work, two data sets are utilized to train and test the above-stated zero-day attack model. The proposed framework specifically includes multiple/several traces of zero-day attacks that are collectively framed in the Datasets –Dataset 1 (Path Dataset) and Dataset 2 (Attack Dataset).

Dataset 1 – Path Simulated Dataset (D1): The dataset is created with CloudSim simulation, where several cloud nodes, virtual machines, and network dependencies are simulated shown in Table 3. It captures interactions of system objects, process dependencies, and the pathways for communications that an attacker could potentially use. The dataset captures many ways that an attacker could exploit the cloud environment, which can be used to form the basis for identifying zero-day attack paths. Features extracted from the data include node connectivity, dependency graphs, and weights of probability of traversals which are significant for mapping out some of the hidden attack paths.

Table 3. Simulation Parameters Table

Parameter	Value
No. of Hosts Simulated	10
OS Environment	Linux (Ubuntu 20.04)
Monitoring Duration	48 hours
No. of Object Instances Captured	~50,000
Avg. Graph Size	8,000 nodes / 25,000 edges
Dependency Types	Read, Write, Execute, Invoke
Noise Filtering	Events < 5 occurrences discarded
Graph Representation	Directed labeled graph

Dataset 2 – Celosia Zero-Day Attack Dataset (D2): This is a benchmark dataset also known as Attack Dataset from Kaggle (Celosia Zero-Day Attack Detection Demo) with 8.14 GB raw data. The dataset is about genuine network traffic traces and the attack logs from cloud hosted services that have suffered various zero-day exploits. It includes a range of features, such as packet headers, protocol metadata, session durations, anomaly scores, and payload signatures. These features can provide insight into unusual changes in normal traffic patterns, which provide strong features to determine and ascertain the possibility of a zero-day attack occurring. Unlike D1, D2 represents real adversarial behavior/adversarial system interactions that can demonstrate the detection capability in realistic situations.

Relevance to Zero-Day Detection: Integrating D1 (attack path simulation) and D2 (real-world attack traces) allows the research work to cover both theorized vulnerability paths and actual adversarial behaviors in a balanced manner. Zero-day attacks are defined as anomaly detections on features critical to an attack, where such features violate the learned definition of how the system behaves legitimately (for example, unusual packet flow, unusual dependency traversals, unseen interactions between processes, etc.). These datasets give full coverage of raw

traffic-based anomalies and attack vector abstraction, suitable for successful training, testing, and online prediction and detection of zero-day attacks.

Phase 2: Enhancing Zero-Day Attack Prediction a Hybrid Game Theory Approach with Neural Networks

Based on the limitations discussed in phase 1 the proposed second phase is to predictively mitigate zero-day attacks before they happen. The traditional methods are conservative, that only react to an intrusion once it has happened, so the objective is to create a predictive model that allows reliable early warning and communication across the cloud infrastructure, built across a hybrid Game Theory model that is grounded in Nash Equilibrium, along with an Adaptive Gaming Model which has a Modified Bi-Directional LSTM (Bi-LSTM), and ANN autoencoder that compress features to decrease duplication. Game-theoretic reasoning models are applied in modeling the attacker-defender interactions, Bi-LSTM applied to account for temporal dependencies in the sequential attack data, providing increased predictive accuracy. Therefore, the proposed model outperformed DT, SVM, GNB, and Logistic Regression by 11.4% in accuracy, 11.3% in precision, 5.5% in recall, and 5.4% in F1 score. This clearly supports predictive capability and provides a high level of communication between the security layers. Results indicate that real-time adjustment of model parameters enhances resistance to adversarial samples and reduces the likelihood of multi-node attacks. Additionally, the learning mechanism, which simulates multi-attacker information sharing, further strengthens the security metric. Overall, the proposed framework demonstrates improved robustness and provides analytical insights into zero-day attack and defense strategies. Phase 2 shows improved prediction, however it does not provide real time detection of an existing, zero-day attack. This progresses to the third phase, and involves developing detection mechanisms using deep convolutional models.

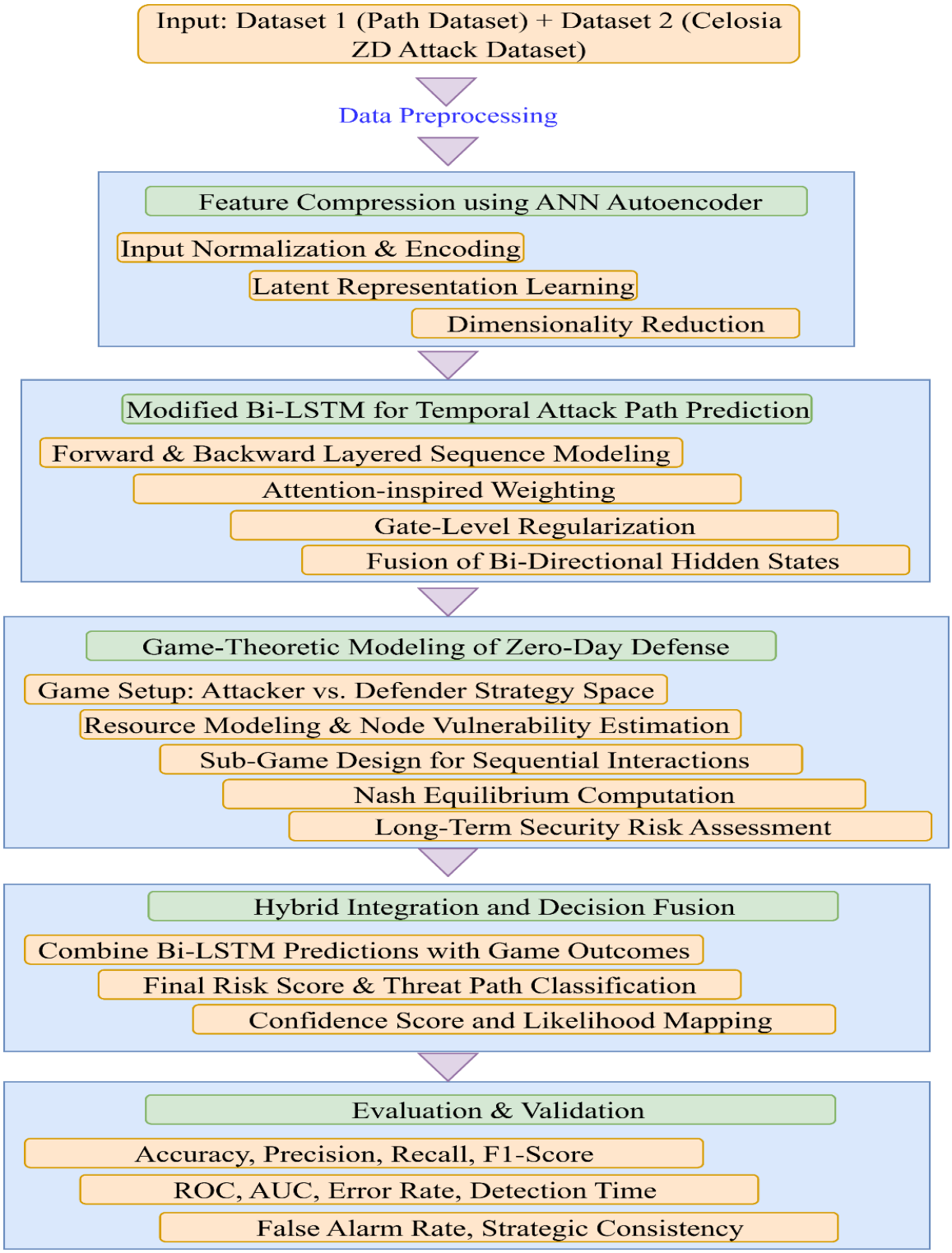
Input: Dataset 1 (Path Dataset) + Dataset 2 (Celosia ZD Attack Dataset)
Data Preprocessing
Feature Compression using ANN Autoencoder
Input Normalization & Encoding
Latent Representation Learning
Dimensionality Reduction
Modified Bi-LSTM for Temporal Attack Path Prediction
Forward & Backward Layered Sequence Modeling
Attention-inspired Weighting
Gate-Level Regularization
Fusion of Bi-Directional Hidden States
Game-Theoretic Modeling of Zero-Day Defense
Game Setup: Attacker vs. Defender Strategy Space
Resource Modeling & Node Vulnerability Estimation
Sub-Game Design for Sequential Interactions
Nash Equilibrium Computation
Long-Term Security Risk Assessment
Hybrid Integration and Decision Fusion
Combine Bi-LSTM Predictions with Game Outcomes
Final Risk Score & Threat Path Classification
Confidence Score and Likelihood Mapping
Evaluation & Validation
Accuracy, Precision, Recall, F1-Score
ROC, AUC, Error Rate, Detection Time
False Alarm Rate, Strategic Consistency

Figure 5. Proposed Framework of Zero-Day Attack Prediction in Phase 2

Figure 5. presents a novel zero-day attack defense framework combining ANN autoencoder-based feature compression with a modified Bi-LSTM for temporal sequence modeling and attention. Game theory is applied to model defender–attacker interactions and

compute Nash equilibrium, enabling risk classification and quantification. The system is evaluated using metrics like accuracy, ROC, and strategic consistency, highlighting its effectiveness.

Table 4. Performance Comparison on Proposed Model for Dataset 1 and 2

Dataset	Algorithm	Accuracy	Precision	Recall	F-measure
Dataset 1 (Path Dataset)	DT	89	89	88	89
	SVM	84	80	86	85
	GNB	90	90	87	89
	LR	84	81	89	85
	Modified Bi-LSTM and Hybrid GT with ANN-AE	**95.4**	**91.3**	**91.5**	**90.4**
Dataset 2 (Attack Dataset)	DT	85	82	83	84
	SVM	85	81	84	86
	GNB	90	84	86	85
	LR	84	81	89	85
	Modified Bi-LSTM and Hybrid GT with ANN-AE	**95**	**90.3**	**90.8**	**89.1**

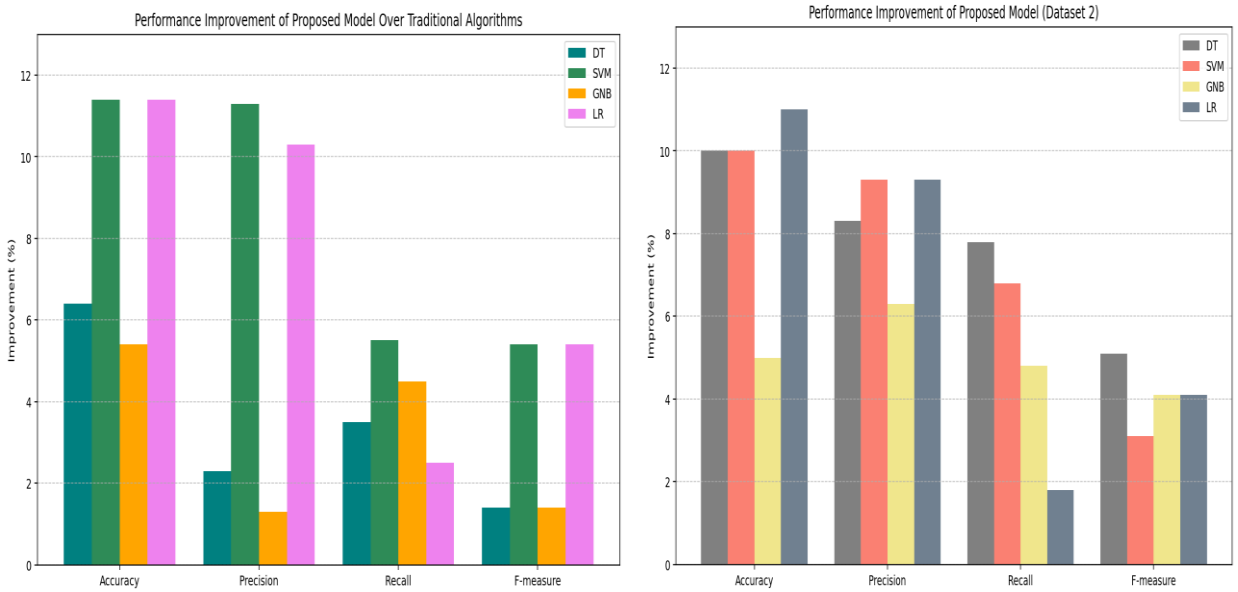

Figure 6. Performance Improvement on Proposed Model Dataset 1 and 2

The Hybrid Game Theory and ANN-Autoencoder Bi-LSTM Modified model consistently outperforms conventional models like SVM, LR, DT, and GNB, with accuracy and precision gains up to 11.5%, particularly over SVM and LR. It proves highly effective in detecting zero-day attacks and maintains strong performance across both datasets. Table 4 and Figure 6, confirm its superiority in all key metrics, with LR showing good improvement in accuracy and DT in recall and F-measure, while GNB lags behind, emphasizing the model's robustness against traditional classifiers. Though the zero-day attacks are predicted to further enhance the model reliability and robustness it is incredibly important to examine various predictive measures which paves way for efficient detection of zero-day attacks.

Phase 3: RESNet50-Based Deep Convolutional Neural Network for Zero-Day Attack Prediction and Detection

Based on the limitations discussed in phase 2 this phase suggests employing a deep convolutional n-zero-day adversarial safety network (DC-nZDASN) that demonstrates a significant improvement in detecting zero-day attacks. This phase of research moves from prediction to real-time, detection of live zero-day attacks. The aim is to limit damage caused by an attack by detecting the anomaly as they occur in a cloud communication traffic stream. A Residual Network based Deep Convolutional Zero-Day Adversarial Safety Network (DC-nZDASN) is proposed. It uses ResNet50 layers, adversarial synthetic data generation, and deep feature learning with Decision Tree Regression and Random Forest Feature engineering. The hybridization ensures the model generalize well across a wider range of possible traffic patterns. Experimental results show that the proposed DC-nZDASN model gained a 12.4% improved detection accuracy against HMM, a maximum of 9.7% accuracy over Bayesian GNN, and significantly higher precision, recall, and F1 metrics than BERT, TransVAE and HADE-SVM for the range of datasets and model variations. The results demonstrate that it meets the original requirements for real time anomaly detection of attacks in cloud networks. Although the Phase 3 research shows improvement on all metrics, given the nature of detection at scale, the research will face even more extensive scalability and optimization issues when used for real-time detection at very large scale. This provides a strong rationale for Phase 4 by applying optimization and ensembles approaches that take advantage of the cloud.

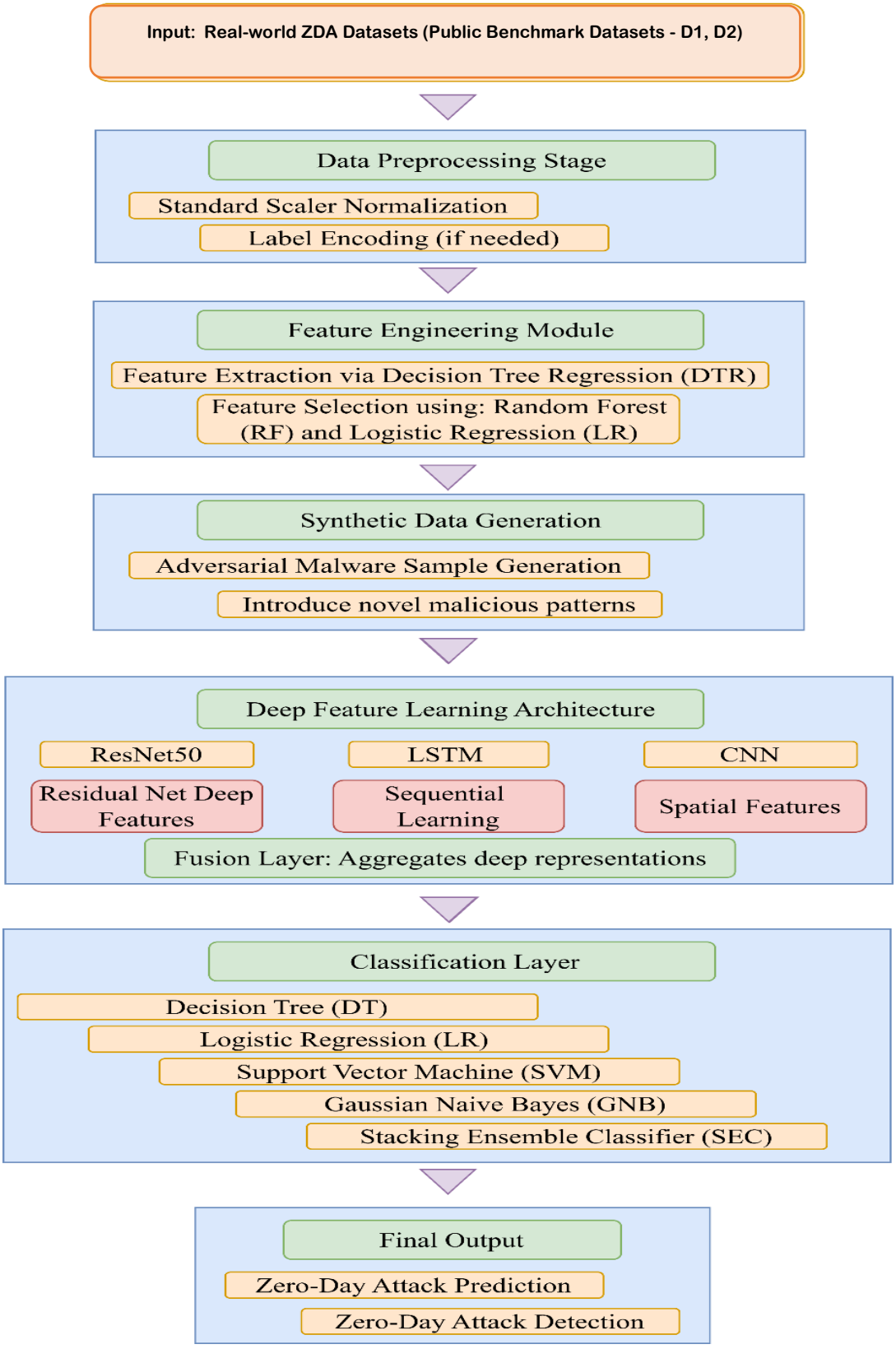

Figure 7. Proposed Framework of Zero-Day Attack Prediction and Detection in Phase 3

Figure 7. Outlines a deep learning pipeline for zero-day attack detection, beginning with data preprocessing, followed by feature engineering using Decision Tree Regression and Random Forest. It incorporates adversarial synthetic data and deep feature learning through ResNet50, LSTM, and CNN to capture complex patterns. The final ensemble classification achieves superior accuracy and enhanced robustness against zero-day attacks compared to existing methods.

Table 5. Performance Comparison for Zero-Day Attack Prediction

Dataset	Model	Accuracy	Precision	Recall	F-Measure
Dataset 1 (Path Dataset)	Hidden Markov Model	84.5	82.1	83.0	82.5
	BERT	89.2	86.8	87.5	87.1
	Modified Bi-LSTM and Hybrid GT with ANN-AE	95.4	91.3	91.5	90.4
	DC-nZDASN	**96.9**	**92.3**	**92.1**	**91.7**
Dataset 2 (Attack Dataset)	Hidden Markov Model	86.3	83.2	84.5	83.8
	BERT	88.5	85.9	86.4	86.1
	Modified Bi-LSTM and Hybrid GT with ANN-AE	95.0	90.3	90.8	89.1
	DC-nZDASN	**96.0**	**91.7**	**91.9**	**90.4**

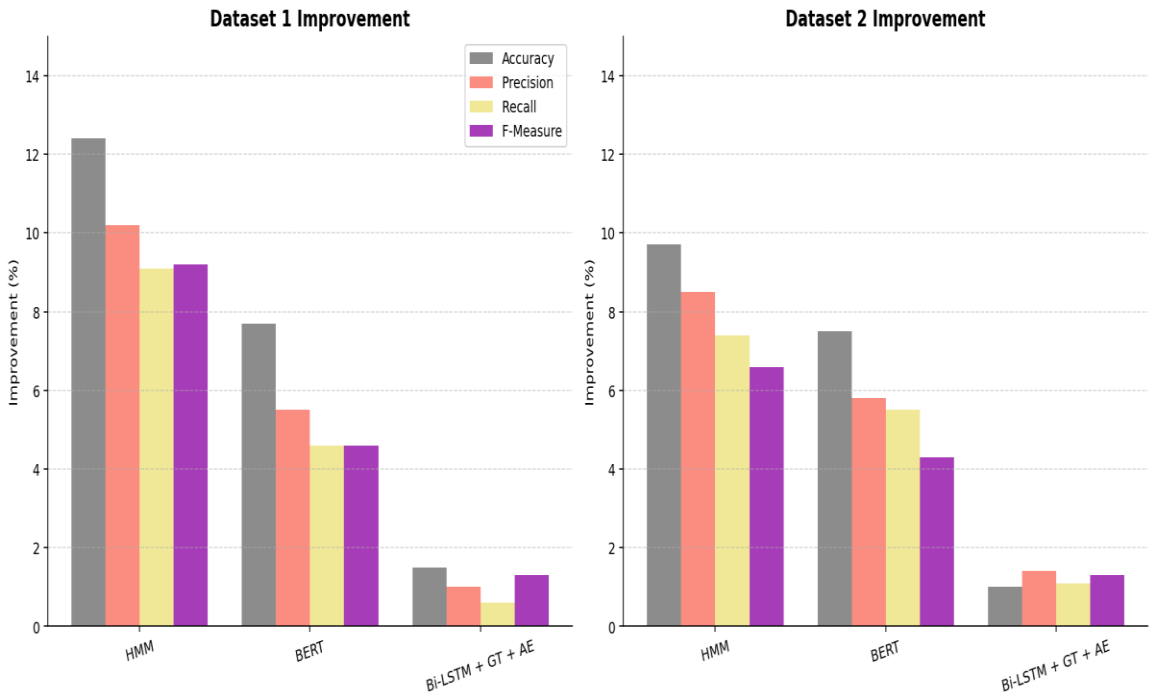

Figure 8. Performance Improvement Chart for Prediction

The proposed DC-nZDASN model outperforms existing methods with significant performance gains, achieving up to +12.4% accuracy over HMM and over +9% in other metrics on Dataset 1. It maintains strong results on Dataset 2, with up to +9.7% improved accuracy and

consistent gains across all evaluation metrics, confirming its effectiveness in detecting zero-day threats. Table 5 and Figure 8, Visualize these improvements across algorithms for both datasets.

Table 6. Performance Comparison for Zero-Day Attack Detection

Dataset	Model	Accuracy	Precision	Recall	F-Measure
Dataset 1 (Path Dataset)	Bayesian GNN	87.2	84.5	85.3	84.9
	TransVAE Threat Detector	89.6	86.7	87.1	86.9
	HADE – One Class SVM	91.3	88.5	89.0	88.7
	DC-nZDASN	**96.2**	**93.1**	**93.8**	**92.7**
Dataset 2 (Attack Dataset)	Bayesian GNN	85.4	83.1	82.6	82.8
	TransVAE Threat Detector	88.8	86.2	85.9	86.0
	HADE – One Class SVM	90.1	87.8	87.4	87.6
	DC-nZDASN	**96.9**	**93.3**	**93.4**	**92.9**

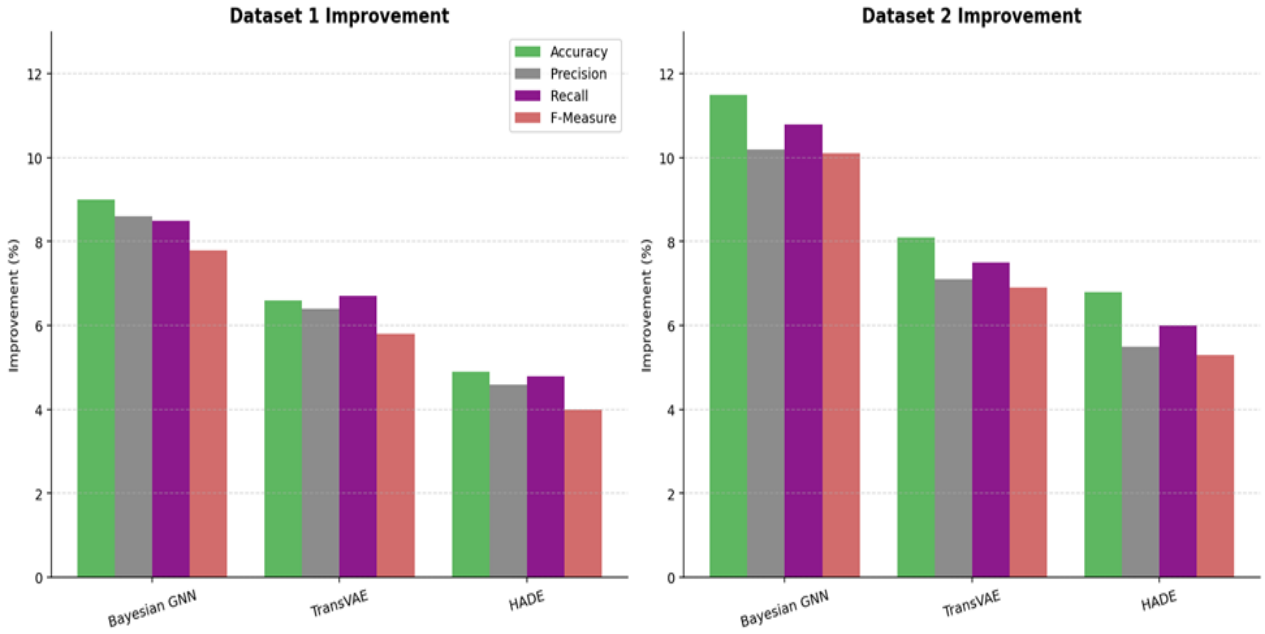

Figure 9. Performance Improvement Chart for Detection

Table 6 and Figure 9. Show that the proposed DC-nZDASN model significantly outperforms Bayesian GNN, TransVAE, and HADE, with up to 9.0% higher accuracy on Dataset 1 and 11.5% on Dataset 2, along with consistent gains in precision, recall, and F-measure. Its strong performance, especially over Bayesian GNN, highlights its robustness in detecting zero-day attacks across diverse architectures. Finding a performance efficient method for zero day attack further leads to a comparative analysis.

Phase 4: Enhancing Cyber Defense against Zero-Day Attacks using Ensemble Neural Networks

The final phase presents the effectiveness and key findings of the research implications. This phase is committed to enhance detection performance and mitigating time complexity

through a solid comparative evaluation across several deep learning models. The aim is to maximize recognition rates while minimizing false positives in large-scale deployments to the cloud. This phase utilizes the Optimized Levy Flight Fruit Fly Optimization Algorithm (OLFFOA) for on-the-fly hyperparameter tuning of deep models such as ResNet50, CNN-LSTM, and Bi-LSTM. Lastly, by utilizing a Stacking Ensemble Classifier for predictions results in more robust and decisive developed model. This stacking ensemble achieved an accuracy of 98.1%, precision of 95.2%, recall of 94.4%, and F1-score of 94.8% on Dataset 2, with each model achieving 1.9%–3.1% lower than the stacking model's metrics. Also, this model performs better than the previously mentioned models in terms of minimizing false positives and reducing detection latency, which also confirms its scalability and reliability. Evaluations conducted on two benchmark datasets validate the effectiveness of the approach, confirming its potential for real-time ZDA detection and broader applications in cybersecurity.

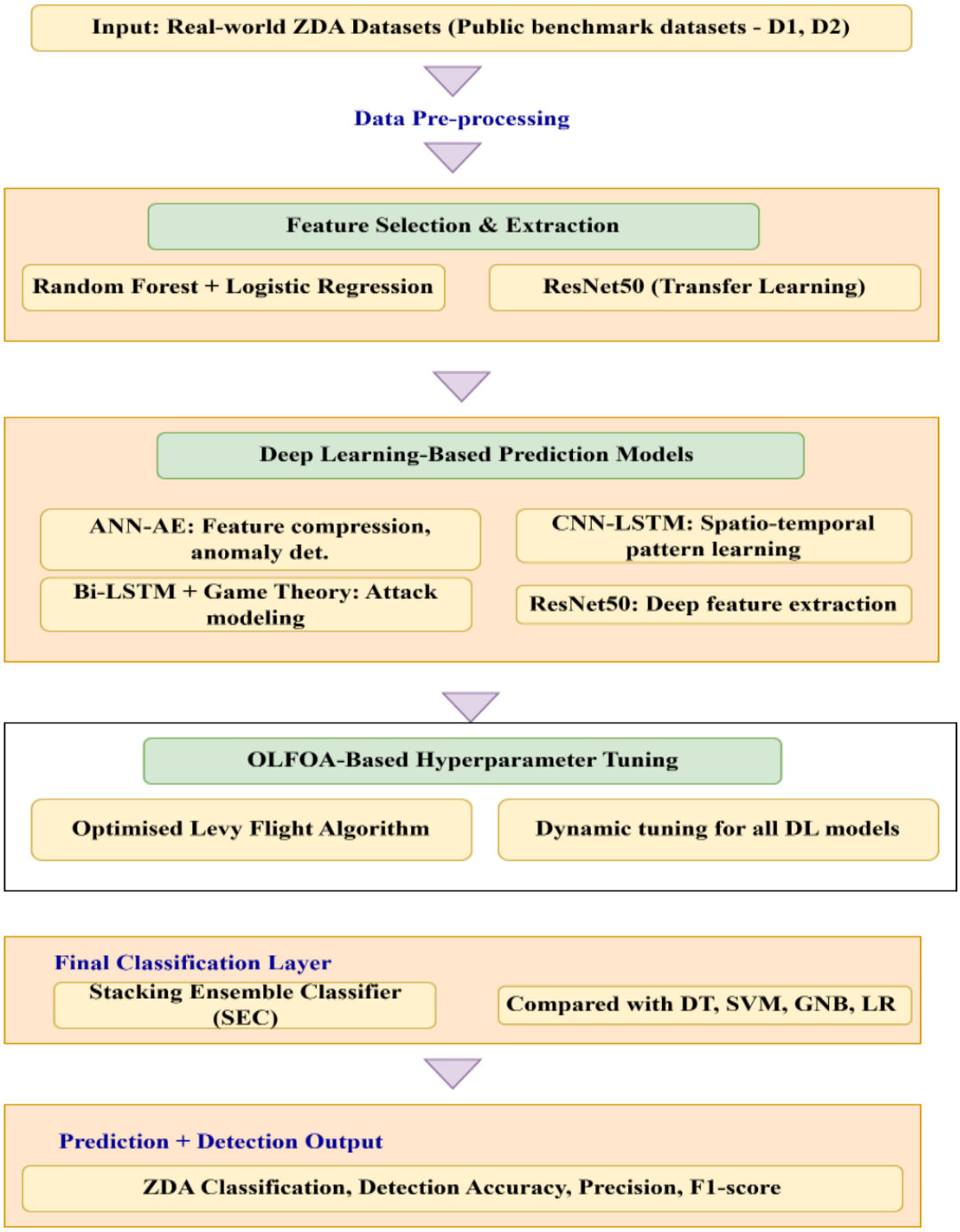
Input: Real-world ZDA Datasets (Public benchmark datasets - D1, D2)
Data Pre-processing
Feature Selection & Extraction
Random Forest + Logistic Regression
ResNet50 (Transfer Learning)
Deep Learning-Based Prediction Models
ANN-AE: Feature compression, anomaly det.
CNN-LSTM: Spatio-temporal pattern learning
Bi-LSTM + Game Theory: Attack modeling
ResNet50: Deep feature extraction
OLFOA-Based Hyperparameter Tuning
Optimised Levy Flight Algorithm
Dynamic tuning for all DL models
Final Classification Layer
Stacking Ensemble Classifier (SEC)
Compared with DT, SVM, GNB, LR
Prediction + Detection Output
ZDA Classification, Detection Accuracy, Precision, F1-score

Figure 10. Proposed Framework of Zero-Day Attack Prediction Comparison in Phase 4

Figure 10, illustrate a complete pipeline for Zero-Day Attack (ZDA) prediction and detection starting with preprocessing of real-world datasets, by applying feature selection based on Random Forest + Logistic Regression and transfer learning based on ResNet50. It employs multiple deep learning models and integrates dynamic hyperparameter tuning through OLFFOA. Finally, a Stacking Ensemble Classifier combines predictions for consistent and accurate ZDA detection.

Table 7. Overall Results

Dataset	Model	Accuracy	Precision	Recall	F1-Score
Dataset 1 (Path Dataset)	ResNet50 + OLFOA	95.9	89.5	88.4	89.0
	CNN-LSTM + OLFOA	96.01	90.2	89.02	90.0
	Bi-LSTM with GT + OLFOA	95.4	89.3	91.5	90.4
	Full Ensemble + OLFOA	**97.8**	**94.5**	**93.7**	**94.1**
Dataset 2 (Attack Dataset)	ResNet50 + OLFOA	95.9	92.3	91.1	91.7
	CNN-LSTM + OLFOA	96.02	93.7	90.04	92.32
	Bi-LSTM with GT + OLFOA	95.0	88.3	89.8	89.1
	Full Ensemble + OLFOA	**98.1**	**95.2**	**94.4**	**94.8**

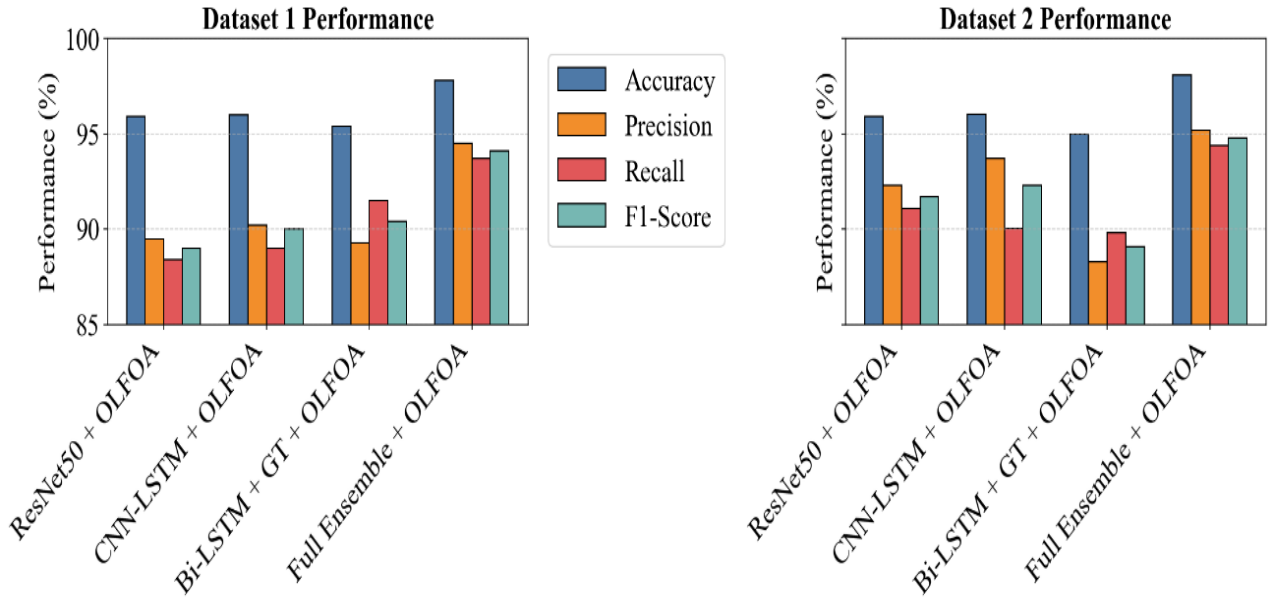

Figure 11. Overall Result Comparison Chart

Table 7 and Figure 11, show that the Full Ensemble + OLFOA model achieves the highest performance across all metrics Accuracy, Precision, Recall, and F1-Score demonstrating superior detection capability. Additionally, Dataset 2 generally performs slightly better or on par with Dataset 1 across most models and metrics, highlighting the model's consistency.

Experimental results of each phases confirms that the innovative methodologies, particularly the BPNN and Stacking Ensemble approaches, are significantly better than most available techniques. In Phase 4, the entire framework and steps integrated into the end-to-end zero-day attack defense mechanism: Path identification, prediction, detection, and the static components of optimization to enhance its practical use in operationalization. The final phase of analysis verifies the validity of the proposed methodologies and suggests the performance efficient methods to handle zero-day attacks in cloud are the most desirable model suitable for practical applicability in real-world scenarios.

9. Summary, Conclusion and Future Scope

In conclusion, this comprehensive research has successfully addressed critical challenges in identifying, predicting, detecting, and optimizing responses to zero-day attacks in dynamic environments such as cloud networks. By introducing a novel proactive approach, the performance efficient methods for handling zero-day attack outlines the techniques used to manage zero-day attacks in the cloud involving path identification, prediction, detection, and optimization. The Enhanced BPNN with probabilistic graphs demonstrated shows better results in identifying attack paths with results of +3.01 accuracy and + 2.34 F1-score compared to Bayesian models in Phase 1. Phase 2 presented a hybrid Game Theory-BiLSTM model with ANN autoencoder compression that outperformed DT, SVM, GNB and LR by up to +11.4% accuracy and +11.3% precision. Phase 3 incorporated ResNet50, CNN, LSTM and adversarial learning, training the DC-nZDASN detection architecture (+12.4% accuracy compared to HMM, and +9.7 compared to Bayesian GNN) and showed better results than BERT, TransVAE and HADE-SVM. Lastly, in Phase 4, the OLFFOA-based hyperparameter tuning is used with an ensemble of ResNet50, CNN-LSTM, and Bi-LSTM, and the best performance is obtained, at 98.1 percent accuracy, 95.2 percent precision, 94.4 percent recollection, and 94.8 percent F1-rank, flags lowered on false appearances and the enhancement of scalability. The proposed method has shown a high level of improvements all around the current techniques, this confirms its effectiveness and resilience in preventing zero-day attacks. The consolidation of machine learning, deep learning, and optimization techniques not only enhances detection robustness but also paves the way for adaptive, scalable, and proactive defense mechanisms against sophisticated zero-day threats. This research contributes significantly to the field of cybersecurity by delivering practical insights and scalable solutions for strengthening digital infrastructures against emerging attacks.

Future research should focus on improving the interpretability of predictive models through explainable AI techniques, addressing privacy concerns with privacy-preserving ML and DL methods, and implementing real-time response mechanisms for threat mitigation. Additionally, establishing standardized benchmark datasets and evaluation protocols could facilitate reproducibility and comparison of results, accelerating research progress in the field. By pursuing these avenues of research, the effectiveness and reliability of zero-day attack can be significantly enhanced, ultimately strengthening cybersecurity defenses against emerging threats.

10. Publications

Journals

- Swathy Akshaya M and Padmavathi G. Zero-day attack path identification using probabilistic and graph approach based back propagation neural network in cloud. Mathematical Statistician and Engineering Applications. 2022; 71.3s2, 1091-1106. (Cited by 10)
- Akshaya S and Padmavathi G. Enhancing zero-day attack prediction a hybrid game theory approach with neural networks. International Journal of Intelligent Systems and Applications in Engineering. 2024; Vol.12, 643-663. (Scopus Indexed, Cited by 6)

- Akshaya S and Padmavathi G. ResNet50-based deep convolutional neural network for zero-day attack prediction and detection. International Journal of Advanced Technology and Engineering Exploration. 2025; Vol.12 (124), 507-527. (Scopus Indexed, Cited by 1)
- Akshaya S and Padmavathi G. Enhancing Cyber Defense Against Zero-Day Attacks Using Ensemble Neural Networks. International Journal of Advanced Technology and Engineering Exploration. 2025, Vol.17 (4). (Scopus Indexed)

Conferences

- Swathy Akshaya, M., Padmavathi, G. (2019). Taxonomy of Security Attacks and Risk Assessment of Cloud Computing. In: Peter, J., Alavi, A., Javadi, B. (eds) Advances in Big Data and Cloud Computing. Advances in Intelligent Systems and Computing, vol 750. Springer, Singapore. (Scopus Indexed, Cited by 34)
- S. A. M and P. G, A Survey on Various Intrusion Detection System Tools and Methods in Cloud Computing, 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2019, pp. 439-445. (Scopus Indexed, Cited by 4)
- M, Swathy Akshaya and G, Padmavathi, A Study on Zero-Day Attacks (2019). Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur – India. (Cited by 4)

Book Chapter

- Swathy Akshaya, M., and Ganapathi, P. (2020). A Review of Machine Learning Methods Applied for Handling Zero-Day Attacks in the Cloud Environment. Handbook of Research on Machine and Deep Learning Applications for Cyber Security, 364-387. (Scopus Indexed, Cited by 9)

11. Significant References

1. Bilge, Leyla and Tudor Dumitraş. "Before we knew it: an empirical study of zero-day attacks in the real world." In Proceedings of the 2012 ACM conference on Computer and communications security, pp. 833-844. 2012.
2. Ratinder Kaur and Maninder Singh, “A Survey on Zero-Day Polymorphic Worm Detection Techniques”, IEEE Communications Surveys and Tutorials, 2014.
3. Ponemon Institute. (2023). Cost of a data breach report 2023. Retrieved from https://www.ibm.com/security/data-breach.
4. Xiaoyan Sun, Jun Dai, Peng Liu, Anoop Singhal and John Yen., “Using Bayesian Networks for Probabilistic Identification of Zero-day Attack Paths”, IEEE Transactions on Information Forensics and Security, 2018, IEEE.
5. Jun Dai, Xiaoyan Sun, and Peng Liu, “Patrol: Revealing Zero-Day Attack Paths through Network-Wide System Object Dependencies”, Springer, 2013.
6. Xiaoyan Sun, Jun Dai, Peng Liu, Anoop Singhal, John Yen, “Towards Probabilistic Identification of Zero-day Attack Paths”, CNS, 2016.
7. Wang et al. “k-Zero Day Safety: A Network Security Metric for Measuring the Risk of Unknown Vulnerabilities”, IEEE Transactions on Dependable and Secure Computing, Volume: 11, Issue: 1, P.no: 30 - 44, 2014.
8. Yuan Ning, Yufeng Liu, Qiang Ji., “Bayesian - BP Neural Network Based Short-term Load Forecasting for Power System”, 3rd International Conference on Advanced Computer Theory and Engineering (1CACTE), 2010, IEEE.

9. Mishra P, Varadharajan V, Tupakula U and Pilli ES. (2018). A Detailed Investigation and Analysis of using Machine Learning Techniques for Intrusion Detection. IEEE Communications Surveys & Tutorials, 1–1.
10. Mikhail Zolotukhin and Timo Hamalainen, “Detection of Zero-day Malware Based on the Analysis of Opcode Sequences” IEEE 11th Consumer Communications and Networking Conference (CCNC),2014.
11. FireEye Mandiant. (2023). 2023 M-Trends report: Insights into todays advanced cyber threats. Retrieved from https://www.fireeye.com.
12. Singh et al. “Zero-day Attacks Detection and Prevention Methods” – Apriorit, 2017.
13. Emmah VT, Ugwu C and Onyejegbu LN. (2021). An Enhanced Classification Model for Likelihood of Zero-Day Attack Detection and Estimation. European Journal of Electrical Engineering and Computer Science, 5(4), 69-75.
14. Scholten CPB. (2021). Automatic detection of zero-day attacks in high-interaction IoT honeypots using static analysis techniques.
15. Soltani, Mahdi, BehzadOusat, Mahdi JafariSiavoshani, and Amir Hossein Jahangir. "An adaptable deep learning-based Intrusion Detection System to zero-day attacks." Journal of Information Security and Applications 76 (2023).